UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/746,015	12/26/2000	Glenn Langford	77666-8/jpw	2269

7380 7590 05/21/2004

SMART & BIGGAR/FETHERSTONHAUGH & CO.
P.O. BOX 2999, STATION D
55 METCALFE STREET
OTTAWA, ON K1P5Y6
CANADA

EXAMINER	
ABRISHAMKAR, KAVEH	

ART UNIT	PAPER NUMBER
2131	5

DATE MAILED: 05/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/746,015	Applicant(s) LANGFORD, GLENN	
	Examiner Kaveh Abrishamkar	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 December 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication field on December 26, 2000. Claims 1 – 42 were received for consideration. No preliminary amendments for the claims were filed. Currently claims 1 – 42 are being considered.

Information Disclosure Statement

2. An initialed and dated copy of Applicant's IDS form 1449, Paper No. 4, is attached to the Office action.

Claim Objections

3. Claim 10 is objected to because of the following informalities: "informations" on line 29 should be changed to "information." Appropriate correction is required.

4. Claim 28 is objected to because of the following informalities: The claim is concluded with a ";" on line 17 and should be concluded with a "." Appropriate correction is required.

5. Claim 35 is objected to because of the following informalities: On line 4, "comprising" should be placed in between the words "further" and "means." Appropriate correction is required.

6. Claim 41 is objected to because of the following informalities: On line 3, the claim limitation is concluded by a "," and should be concluded with a ";". Appropriate correction is required.

7. Claim 12 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. The decryptor that implements the method of claim 1 is not a proper depended claim as it does not further limit the parent claim 1.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 13-30 and 38-42 are rejected under 35 U.S.C. 102(b) as being anticipated by Ford et al. (U.S. Patent 5,481,613).

Regarding claim 13, Ford discloses:

A key release method comprising:

receiving a key ciphertext and key related information in respect of a key used to encrypt the key ciphertext from a decryptor (Figure 2, column 6 lines 24 – 40);

obtaining decryptor information in respect of the decryptor (column 6 lines 42 – 65); and

deciding based on the decryptor information and the key related information whether decryption of the key ciphertext is to be permitted (column 6 lines 56 – 66).

Regarding claim 29, Ford discloses:

A method of controlling access to a decryption key comprising:

receiving from a decryptor a key release request comprising decryptor information and the decryption key encrypted using a public key (Figure 2 step 34, column 6 line 40 – column 7 line 49);

applying decryption authorization logic associated with the public key used to encrypt the decryption key to the decryptor information to determine whether the decryptor should be permitted access to the decryption key (column 7 lines 35 – 49);

upon determining the decryptor should be permitted access to the decryption key, sending a key release response specifying the decryption key (column 7 lines 35 – 49).

Regarding claim 30, Ford discloses:

A method of controlling access to decryption keys comprising:

maintaining a private key repository comprising a plurality of access identifiers, and for each access identifier at least one key related information of a respective {public key, private key} pair, the repository also containing the private key of each {public key, private key} pair (column 5 line 26 – column 6 line 33);

maintaining a repository comprising for each access identifier a respective decryptor authorization logic which can be applied to a decryptor information (Figure 2, (column 5 line 26 – column 6 line 4, column 6 lines 48 – 55);

obtaining decryptor information (Figure 2 step 34, column 6 line 40 – column 7 line 49);

receiving a key release request containing a decryption key encrypted using a public key of a {public key, private key} pair and containing a key related information associated with the (public key, private key} pair (column 7 lines 35 – 49);

for each access identifier in association with which the key related information is stored, applying the respective decryptor authorization logic to the decryptor information specified in the key release request (column 7 lines 35 – 49);

in the event the decryptor information satisfies at least one of the respective decryptor authorization logics, decrypting the ciphertext to recover the decryption key, and sending a key release response to the decryptor specifying the decryption key (column 7 lines 35 – 49).

Regarding claim 38, Ford discloses:

A key release agent comprising:

means for receiving from a decryptor a key ciphertext and key related information in respect of a key used to encrypt the key ciphertext (Figure 2 step 34, column 6 line 40 – column 7 line 49);

means for obtaining decryptor information in respect of the decryptor (Figure 2 step 34, column 6 line 40 – column 7 line 49);

means for deciding based on decryptor information of the decryptor and the key related information whether decryption of the key ciphertext is to be permitted (column 7 lines 35 – 49).

Claim 14 is rejected as applied above in rejecting claim 13. Furthermore, Ford discloses:

A method according to claim 13 wherein the decryptor information is received from the decryptor together with the key ciphertext and key related information (Figure 2 step 34, column 6 line 40 – column 7 line 49).

Claim 15 is rejected as applied above in rejecting claim 13. Furthermore, Ford discloses:

A method according to claim 13 wherein obtaining decryptor information comprises receiving the decryptor information while establishing a secure connection with the decryptor (Figure 2 step 34, column 6 line 40 – column 7 line 49).

Claim 16 is rejected as applied above in rejecting claim 13. Furthermore, Ford discloses:

A method according to claim 13 wherein obtaining decryptor information comprises:

receiving from the decryptor a decryptor identifier (Figure 2 step 34, column 6 line 40 – column 7 line 49);

using the decryptor identifier to lookup decryptor attributes from a public repository, the decryptor identifier and decryptor attributes together constituting the decryptor information (Figure 2, column 6 line 42 – 65).

Claim 17 is rejected as applied above in rejecting claim 13. Furthermore, Ford discloses:

A method according to claim 13 further comprising:

using information in a certificate as the decryptor information (column 6 lines 42 – 55).

Claim 20 is rejected as applied above in rejecting claim 13. Furthermore, Ford discloses:

A method according to claim 13 wherein the decryptor information is an identity or role of the decryptor, an alias, or a claim of access rights or privilege, or some other attribute of the decryptor of a corresponding decrypting device or platform (column 6 line 40 – column 7 line 49).

Claim 21 is rejected as applied above in rejecting claim 13. Furthermore, Ford discloses:

A method according to claim 13 wherein the key related information comprises a key pair identifier (column 5 line 18 – column 6 line 32).

Claim 22 is rejected as applied above in rejecting claim 13. Furthermore, Ford discloses:

A method according to claim 13 further comprising:

decrypting the key ciphertext, re-encrypting the key using a public key of a {public key, private key} pair to produce a re-encrypted key, the private key of which is available to the decryptor, and sending the re-encrypted key to the decryptor (column 7 lines 8 – 49).

Claim 23 is rejected as applied above in rejecting claim 13. Furthermore, Ford discloses:

A method according to claim 13 further comprising:

decrypting the key ciphertext to obtain a decryption key (Figure 4, column 7 lines 35 – 50);

sending the decryption key to the decryptor over a secure channel (Figure 4, column 7 lines 35 – 50).

Claim 24 is rejected as applied above in rejecting claim 13. Furthermore, Ford discloses:

A method according to claim 13 further comprising:

decrypting the key ciphertext to obtain a decryption key (Figure 4, column 7 lines 35 – 50);

using a symmetric key available to the decryptor, encrypting the decryption key with the symmetric key to produce an encrypted decryption key, and sending the encrypted decryption key to the decryptor (Figure 4, column 7 lines 35 – 50).

Claim 25 is rejected as applied above in rejecting claim 13. Furthermore, Ford discloses:

A method according to claim 13 further comprising:

receiving a plurality of key ciphertexts and respective key related information from the decryptor and determining whether at least one private key required to decrypt a respective at least one key ciphertext of the plurality of key ciphertexts is available (Figure 2, column 6 lines 24 – 40);

upon determining such at least one private key is available, deciding based on the decryptor information whether decryption of at least one of the plurality of key ciphertexts is to be permitted (column 7 lines 35 – 49).

Claim 28 is rejected as applied above in rejecting claim 13. Furthermore, Ford discloses:

A method according to claim 13 wherein deciding based on decryptor information of the decryptor and the key related information whether decryption of the key ciphertext is to be permitted comprises applying at least one rule associated with the public key used to encrypt the decryption key to the decryptor information to determine whether the decryptor should be permitted access to the decryption key (column 7 lines 35 – 49).

Claim 39 is rejected as applied above in rejecting claim 38. Furthermore, Ford discloses:

A key release agent according to claim 38 adapted to receive the decryptor information together with the key ciphertext and key related information (Figure 2, column 6 lines 24 – 40).

Claim 40 is rejected as applied above in rejecting claim 39. Furthermore, Ford discloses:

A key release agent according to claim 38 adapted to use the decryptor identifier to lookup decryptor attributes from a repository, the decryptor identifier and decryptor attributes together constituting the decryptor information (Figure 2, column 6 line 42 – 65).

Claim 41 is rejected as applied above in rejecting claim 38. Furthermore, Ford discloses:

A key release agent according to claim 38 further comprising:
decrypting means for decrypting the key ciphertext (column 7 lines 8 – 49).
encryption means for re-encrypting the key using a public key of a {public key, private key pair to produce a re-encrypted key, the private key of which is available to the decryptor (column 7 lines 8 – 49);
means for sending the re-encrypted key to the decryptor (column 7 lines 8 – 49).

Claim 42 is rejected as applied above in rejecting claim 38. Furthermore, Ford discloses:

A key release agent according to claim 38 further comprising:
decryptor authorization logic associated with each public key used to encrypt the decryption key to the decryptor information for determining whether the decryptor should be permitted access to the decryption key (column 7 lines 35 – 49).

Claim 18 is rejected as applied above in rejecting claim 17. Furthermore, Ford discloses:

A method according to claim 17 further comprising:

obtaining the certificate from a certificate repository (column 6 lines 42 – 55).

Claim 19 is rejected as applied above in rejecting claim 17. Furthermore, Ford discloses:

A method according to claim 17 further comprising receiving the certificate together with the key ciphertext and key related information (column 6 lines 42 – 55).

Claim 26 is rejected as applied above in rejecting claim 25. Furthermore, Ford discloses:

A method according to claim 25 further comprising:

decrypting one of the key ciphertexts using a corresponding private key to recover a decryption key (Figure 2, column 6 lines 24 – 40).

Claim 27 is rejected as applied above in rejecting claim 25. Furthermore, Ford discloses:

A method according to claim 25 wherein deciding based on decryptor information of the decryptor and the key related information whether decryption of at least one of the key ciphertexts is to be permitted comprises applying decryptor authorization logic associated with each public key used to encrypt the decryption key to the decryptor

information to determine whether the decryptor should be permitted access to the decryption key (column 7 lines 35 – 49).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1 – 12 and 31 – 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ford et al. (U.S. Patent 5,481,613).

Regarding claim 1, Ford discloses:

A method for a decryptor to obtain a decryption key from a key release agent comprising:

a decryptor obtaining an encryption block comprising a data ciphertext requiring a decryption key to decrypt, the encryption block further comprising key related information associated with a first (public key, private key) pair, the encryption block further comprising a key ciphertext consisting of the decryption key encrypted by the first public key of the first {public key, private key) pair (Figure 2 step 34, column 6 line 40 – column 7 line 49);

the decryptor generating a key release request containing the key ciphertext, and the key related information and outputting the key release request to the key release agent (Figure 2 step 34, column 6 line 40 – column 7 line 49);

the decryptor receiving a key release response specifying the decryption key (column 7 lines 35 – 49).

Ford however discloses that the encryption block includes an access controlled decryption block (ACD). However, the use of the ACD is not necessary to the operation of the key release agent releasing the decryption key to a decryptor. The ACD is just another section of data, which cannot be altered without the use of a key release agent (KRA). The exclusion of the ACD does not prohibit the cited prior art from providing a decryptor obtaining an encryption block with key related information, the decryptor generating a key release request, or the decryptor receiving a key release response specifying the decryption key which the claims delineate. Therefore it would have been obvious to one of ordinary skill in the art to exclude the use of the specific data structure designated as the ACD, and replace it with another data structure that just provides key related information and not the additional information associated with the ACD.

Regarding claim 31, Ford discloses a private key repository with key related information and associated private keys of a {public key, private key} pair and a decryptor authorization logic definition function adapted to allow the definition of decryptor authorization logic to be applied to decryptor information to determine eligibility to

decrypt, and for each decryptor authorization logic to select one or more of the key related information in respect of which the rule is to be applied (column 7 lines 35 – 49). Ford does not explicitly disclose an administrative interface comprising a private key maintenance function adapted to allow adding and deleting of a key related information and associated private key of a {public key, private key} pair. However, Ford discloses that the private key and key related information are stored in databases and/or in a trusted server system (column 5 lines 22 – 35). Servers by nature have an administrative interface to manage data, which the keys and key related information are classified. Therefore the function of adding and deleting data (private key and key related information) is a normal function of a server system. Therefore it would have been obvious to one of ordinary skill in the art to incorporate the function of adding and deleting keys and key related data using the server system to achieve the benefits of increased security of the keys and keeping more recent keys. Also, if one key is corrupted or discovered by a third party, it is obvious that the compromised key must be deleted and another must be added in its place. Therefore though not mentioned explicitly in the prior art, the function claimed is deemed obvious in view of the above arguments.

Regarding claim 33, Ford discloses:

A decryptor comprising:

means for obtaining an encryption block comprising a data ciphertext requiring a decryption key to decrypt, the encryption block further comprising key related

information associated with a first {public key, private key pair, the encryption block further comprising a key ciphertext consisting of the decryption key encrypted by the first public key of the first (public key, private key) pair (Figure 2 step 34, column 6 line 40 – column 7 line 49);

means for generating a key .release request containing the key ciphertext, and the key related information and outputting the key release request to the key release agent (Figure 2 step 34, column 6 line 40 – column 7 line 49);

means for receiving a key release response specifying the decryption key (column 7 lines 35 – 49).

Ford however discloses that the encryption block includes an access controlled decryption block (ACD). However, the use of the ACD is not necessary to the operation of the key release agent releasing the decryption key to a decryptor. The ACD is just another section of data, which cannot be altered without the use of a key release agent (KRA). The exclusion of the ACD does not prohibit the cited prior art from providing a decryptor obtaining an encryption block with key related information, the decryptor generating a key release request, or the decryptor receiving a key release response specifying the decryption key which the claims delineate. Therefore it would have been obvious to one of ordinary skill in the art to exclude the use of the specific data structure designated as the ACD, and replace it with another data structure that just provides key related information and not the additional information associated with the ACD.

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Ford discloses:

A method according to claim 1 further comprising the decryptor making the decryptor information available to the key release agent (column 6 lines 42-65).

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Ford discloses:

A method according to claim 1 further comprising the decryptor using the decryption key to decrypt the data ciphertext (Figure 4, column 7 lines 35 – 50).

Claim 6 is rejected as applied above in rejecting claim 1. Furthermore, Ford discloses:

A method according to claim 1 further comprising the decryptor making the decryptor information available to the key release agent by providing a decryptor identifier which may be used to look up decryptor attributes from a repository (Figure 2 step 34, column 6 line 40 – column 7 line 49).

Claim 7 is rejected as applied above in rejecting claim 1. Furthermore, Ford discloses:

A method according to claim 1 wherein the key related information comprises a key pair identifier (column 7 lines 35 – 49).

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, Ford discloses:

A method according to claim 1 further comprising:

before generating the key release request, the decryptor determining if the private key of the first {public key, private key} pair is available at the decryptor (column 6 lines 33 – 65);

upon determining the private key of the first {public key, private key} pair is not available at the decryptor generating the key release request (column 6 lines 33 – 65).

Claim 9 is rejected as applied above in rejecting claim 1. Furthermore, Ford discloses:

A method according to claim 1 further comprising:

decrypting at least a portion of the key release response containing an encrypted version of the decryption key using a private key of a second {public key, private key} pair to recover the decryption key (Figure 4, column 7 lines 35 – 50).

Claim 10 is rejected as applied above in rejecting claim 1. Furthermore, Ford discloses:

A method according to claim 1 wherein the encryption block comprises a plurality of key related information associated with a respective plurality of first {public key, private key} pairs, and a respective plurality of key ciphertexts each consisting of the decryption key encrypted by the public key of a respective one of the plurality of first {public key, private key} pairs associated with the plurality of key related information, the method comprising:

generating the key release request containing the plurality of key ciphertexts, and the associated plurality of key related information (Figure 2 step 34, column 6 line 40 – column 7 line 49).

Claim 12 is rejected as applied above in rejecting claim 1. Furthermore, Ford discloses:

A decryptor adapted to implement a method according to claim 1 (Figure 2 item 30, column 6 line 40 – column 7 line 49).

Claim 32 is rejected as applied above in rejecting claim 31. Furthermore, Ford discloses:

An administrative interface according to claim 31 wherein the private key repository maintenance function is further adapted to store the key related information and associated private key of a public key, private key} pair in association with one of a plurality of access identifiers (column 5 line 26 – column 6 line 33); and

wherein the decryptor authorization logic definition function is further adapted to store each authorization logic in association with one of the plurality of access identifiers (column 7 lines 35 – 49).

Claim 34 is rejected as applied above in rejecting claim 33. Furthermore, Ford discloses:

A decryptor according to claim 33 further comprising means for making the decryptor information available to the key release agent (column 6 lines 42-65).

Claim 35 is rejected as applied above in rejecting claim 33. Furthermore, Ford discloses:

A decryptor according to claim 33 further comprising means for using the decryption key to decrypt the data ciphertext (Figure 4, column 7 lines 35 – 50).

Claim 36 is rejected as applied above in rejecting claim 33. Furthermore, Ford discloses:

A decryptor according to claim 33 adapted to make the decryptor information available to the key release agent by including the decryptor information in the key release request (Figure 2 step 34, column 6 line 40 – column 7 line 49).

Claim 37 is rejected as applied above in rejecting claim 33. Furthermore, Ford discloses:

A decryptor according to claim 33 further comprising means for decrypting at least a portion of the key release response containing an encrypted version of the decryption key using a private key of a second {public key, private key} pair to recover the decryption key (Figure 4, column 7 lines 35 – 50).

Claim 4 is rejected as applied above in rejecting claim 2. Furthermore, Ford discloses:

A method according to claim 2 wherein the decryptor making the decryptor information available to the key release agent comprises including the decryptor information in the key release request (Figure 2 step 34, column 6 line 40 – column 7 line 49).

Claim 5 is rejected as applied above in rejecting claim 2. Furthermore, Ford discloses:

A method according to claim 2 wherein the decryptor making the decryptor information available to the key release agent comprises the decryptor providing the decryptor information to the key release agent while establishing a secure connection with the key release agent (Figure 2 step 34, column 6 line 40 – column 7 line 49).

Claim 11 is rejected as applied above in rejecting claim 10. Furthermore, Ford discloses:

A method according to claim 10 further comprising:

before generating the key release request, determining if at least one private key of the plurality of first {public key, private key} pairs is available at the decryptor (column 6 lines 33 – 65);

upon determining none of the private keys of the plurality of first {public key, private key} pairs is available at the decryptor generating the key release request (column 6 lines 33 – 65).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 703-305-8892. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

KA
05/14/04

Emmanuel L. Moise
EMMANUEL L. MOISE
PRIMARY EXAMINER
A/U 2136